ABSTRACT
ADSTRACT

Methods and apparatus for key distribution in a conditional access system,
assuming that the set of all user nodes which the system can accommodate is a complete
set, and a subset is composed of all user nodes or part of user nodes. One method
comprises: decomposing said subset into at least one secondary subset; assigning a
different user key to each secondary subset, each said user key being transmitted to all
users in a corresponding secondary subset; encrypting an entitlement key by using each
said user key so as to generate a cipher text corresponding to each said secondary subset;
and combining said cipher text to generate a media key control block and transmitting
said media key control block to all users in said subset. Since a classification method of a
binary tree and a multiple tree is used, the invention can save a lot of network resources.